PATCHING THE WETWARE:

ADDRESSING THE HUMAN FACTOR IN INFORMATION SECURITY

GRADUATE RESEARCH PROJECT

Alexander D. Nelson

AFIT/ICW/ENG/11-11

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ICW/ENG/11-11

PATCHING THE WETWARE: ADDRESSING THE HUMAN FACTOR IN INFORMATION SECURITY

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Alexander D. Nelson

June 2011

AFIT/ICW/ENG/11-11

PATCHING THE WETWARE: ADDRESSING THE HUMAN FACTOR IN INFORMATION SECURITY

Alexander D. Nelson

Approved:

_____/signed_____	23 May 2011
Robert F. Mills, PhD (Chairman)	Date
_____/signed_____	23 May 2011
Michael R. Grimaila, PhD, ASM, CISSP (Member)	Date

Abstract

In the practice of information security, it is increasingly observed that the weakest link in the security chain is the human operator. A reason often cited for this observation is that the human operator is simpler and cheaper to manipulate than the complex technological protections of today's digital information systems.

Current events where the human factor was targeted to undermine military information protection systems include the 2008 breach of USCENTCOM computer systems with a USB device, the 2010 Stuxnet software worm launched against Iranian nuclear facilities, and the 2010 compromise of classified documents published to the WikiLeaks website. These infamous anecdotes highlight the need for more robust human-centric information security methods to mitigate the risks of social engineering; the practice of using deceptive psychological methods to influence the human user.

In addressing this need, this research effort analyzes the psychological foundations of social engineering that enable its success. After these enablers have been identified, a qualitative analysis is used to formally demonstrate a link between those psychological foundations and a body of research on persuasion. Once this connection is established, several psychological theories on building resistance to persuasive attempts are presented as novel approaches to defending individuals from the threat of social engineering. Specifically, the application of inoculation, forewarning, metacognition, and dispelling the illusion of invulnerability are discussed.

To Ted

Blue Skies…

Acknowledgements

Very rarely does research occur as the result of one person's effort, and this work is no exception. Most importantly, I want to recognize my family for their support in my decision to return to school and their support throughout my time at AFIT which required the sacrifice of my time spent away from them. Without my wife who took on additional responsibilities with our children, this work would not have been possible. Thank you. I would also like to thank my daughter and son, who as young people with a curiosity of the unknown and a genuine enthusiasm for learning new things have provided me a perfect reminder of what being a research scientist is all about.

I would like to thank my AFIT sponsor and research advisor Dr. Bob Mills, first for believing a behavioral scientist may add value to a computer engineering program, and secondly for providing his expertise and guidance for this research. In the same regard, I would like to thank my professor and research advisor Dr. Michael Grimaila who provided me with a foundational understanding of information security concepts and additional guidance during this work.

Lastly, I would like to thank the classmates who I spent this academic journey with. By observing these eleven other Air Force Majors over the course of a year, I have a new understanding of what "Integrity First, Service Before Self, Excellence in All We Do" truly means. In addition to providing an ideal model of what military officers should be, they never let the token civilian (TC) feel like a token civilian. Thanks!

Table of Contents

List of Figures

Patching the Wetware: Addressing the Human Factor in Information Security

I. INTRODUCTION

"In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control…This previously classified incident was the most significant breach of U.S. military computers ever, and it served as an important wake-up call"

–William J. Lynn III, U.S. Deputy Secretary of Defense (2010)

1.1 Background

Within the purview of information security it is becoming increasingly evident that the weakest link in the security chain is the human user. The reason for this is that the human factor has become simpler and cheaper to manipulate than penetrating the complex technological protections of digital information systems. There have been several current events that exhibit how human operators undermined technological information protection systems of both the United States and foreign militaries. Some of

the most infamous examples include the 2008 breach of USCENTCOM computer systems exposing sensitive data to foreign intelligence, the 2010 Stuxnet software worm launched against Iranian nuclear Supervisory Control and Data Acquisition (SCADA) systems, and the 2010 publication of classified government documents to the WikiLeaks website (Lynn, 2010; Markoff, 2011; Savage, 2010).

In the first of these scenarios, a common social engineering technique known as "baiting" or planting a "road apple" was used to get malicious code onto protected computer systems where the adversary did not have physical access to the targeted systems. In this attack, the road apple consisted of a USB flash drive containing malware planted where someone with physical access to the CENTCOM network would find it (Lynn, 2010). The engineer of this attack relied upon known attributes of human behavior and intentionally manipulated those attributes in order to subvert the information security protection mechanisms in place that otherwise prevented access.

In the case of the 2010 Stuxnet worm that infected Iranian nuclear SCADA systems, investigators have implicated two attack vectors used to infiltrate these systems, both of which relied on the human element to circumvent technological barriers. To this end, The New York Times stated that "Symantec researchers determined that 12,000 infections could be traced back to just five initial infection points" and that "the first step in the infections was either an infected e-mail sent to an intended victim or a hand-held USB device that carried the attack code" (Markoff, 2011).

Similarly, WikiLeaks leader Julian Assange relied upon, and is alleged to have manipulated the human operator to gain access to protected information he was otherwise restricted from. Highlighting this point, an article published in The New York Times

states that “Justice Department officials are trying to find out whether Mr. Assange encouraged or even helped the Army intelligence analyst, Private First Class Bradley Manning, to extract classified military and State Department files from a government computer system” (Savage, 2010). The article goes on to say that “Private Manning is said to claim that he had been directly communicating with Mr. Assange using an encrypted Internet conferencing service as the soldier was downloading government files” (Savage, 2010).

As evidenced by these now infamous anecdotes, securing the “wetware” or human element of an enterprise information system rivals the importance of securing the hardware or software in terms of potential consequence, and may require even more dynamic solution sets.

1.2 Issue: The Increasing Threat of Social Engineering

Social engineering as it is understood in the domain of information security is the practice of using deceptive social and psychological methods on the human element in order to obtain protected information, obtain access, or influence behavior toward those objectives (Mitnick, 2003; Pipkin, 2000; Thornburgh, 2005). It is a very low cost of entry, high payoff means of gaining access to information usually guarded by expensive, complex technological protections. Within the context of our rapidly developing cyber-infrastructure, social engineering presents an asymmetric attack methodology that threatens information security; the practice of protecting information systems and providing information integrity, confidentiality, and availability (Pipkin, 2000).

Because social engineering is an attack vector with such a low cost of entry, many indicators show that the occurrences of its employment are increasing in step with the development of the cyber landscape. To this end, Deputy Secretary of Defense William J. Lynn stated that "Over the past ten years, the frequency and sophistication of intrusions into U.S. military networks have increased exponentially. Every day, U.S. military and civilian networks are probed thousands of times and scanned millions of times" (Lynn, 2010).

As the cyber infrastructure has continued to grow and evolve, so have the development of hardware and software security mechanisms, seemingly at the expense of ignoring the human decision maker in the loop. A 2008 Microsoft Security Intelligence Report states that "improvements in software development practices and the increased availability and awareness of automatic software update mechanisms have greatly limited the kinds of technical exploit opportunities that are available to attackers. Instead, most attackers today rely heavily on social engineering techniques to mislead victims into unwittingly or even knowingly giving them information and access that would be much harder to take by force" (pg 15). To achieve the objective of creating a resilient enterprise information state within our military and private industry alike, more robust considerations must be made for mitigation strategies to user-based threats.

1.3 Implications: The Need for Human-Centric Information Security

Widely recognized information security expert and noted author Donald Pipkin puts forth that "we are standing on the precipice of a new world economy based on information" and that "the top of the Fortune 500 list is full of corporations who do not

build with sweat and steel, but instead have made their fortunes by the application of information" (2000, p. 1). In addition, he states that "Information security is more than computer data security. It is the process of protecting the intellectual property of an organization. This intellectual property is paramount to the organization's survival" (2000, p. xix).

These ideas put forth by Pipkin are no more evident than in the case of military organizations such as the U.S. Air Force which relies on information superiority to successfully complete its mission. Air Force Doctrine Document 2-5 Information Operations, states that "Information superiority is a degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. Information superiority is a critical part of air and space superiority, which gives the commander freedom from attack, freedom to maneuver, and freedom to attack" (2005, p. 1).

With this global shift towards an information-based economy, it has been argued by many that an enterprise's most valuable asset, aside from its people, is its information. Logically following, organizations should develop protection strategies commensurate with the value of that information. It is the author's belief that both the greatest threat to information security and its greatest asset is the human factor, and as such merits the resources and consideration needed to develop vigorous human-centric information security methods. To develop these types of robust mitigations to social engineering threats, we must first develop an understanding about the underlying psychological aspects of social engineering tactics that enable their success.

1.4 Purpose Statement

This research effort is a practical investigation into the emerging threat of social engineering within our evolving cyber infrastructure and the subsequent consequences that threat has on information security. This project analyzes the psychological foundations of social engineering in an attempt to bring about a novel approach to defending individuals and organizations from this threat. Specifically, this research was defined by the research question "How can the Air Force protect its personnel from the increasing information security threat of social engineering such as in the case of the 2008 CENTCOM breach?" In the process of trying to answer this initial research question, several other investigative questions arose and together became the guiding framework for this effort.

The primary purpose of this research then is to formally demonstrate a link between those psychological foundations that enable the success of social engineering techniques and a body of research pertaining to persuasion. If this relationship can in fact be formalized, a secondary purpose for this research will be to discuss how some specific theories developed by social psychologists on the resistance to persuasion could be applied to combat the social engineering threat. In addition to answering these research objectives, it is the author's intent to use this investigation as an emergent theory building exercise for producing testable hypotheses for follow-on experimental studies.

1.5 Scope and Generalizability

The overarching objective of this effort was to develop a novel research perspective for a practical problem experienced by our Air Force by integrating two

fields of study from which the author has received educational training, behavioral science and cyber warfare. In the process of developing the ideas for this research, the author relied heavily on this training and his experience as a research psychologist. The scope and biases of this work are therefore commensurate with those areas of study.

It is important to note here that the current research has an intended application primarily for Air Force personnel. While recognizing this fact, it became obvious through the course of conducting an extensive literature review that the information security threats addressed in this project do not constitute problems that are unique to the Air Force or even the military community in general. Logically following, the findings and propositions in this research could be carefully inferred to other enterprises that rely on information as a central component to their business strategy.

1.6 Organization

This research project was accomplished in several distinct phases that build upon one another and are laid out over the five following chapters of this report. The initial effort is documented in Chapter II and presents a detailed literature review on social engineering. This review is based upon knowledge mined from the information security literature as well as a review of associated constructs detailed in the social psychology literature. This review aims to provide a foundational understanding of social engineering techniques and the psychological underpinnings of those tactics. This review is then used as the underlying input to a qualitative analysis performed during the research process.

Chapter III sets the stage for conducting an analysis of the concepts captured in the literature review by presenting the methodology to be used. Specifically, this chapter presents the general inductive approach as a validated method to make qualitative analyses about concepts such as those found in this research.

Logically following, Chapter IV ties the previous two chapters together by detailing the qualitative analysis performed on two frameworks that were identified during the first phase of the research. The objective of this chapter is to formally establish a relationship between the psychological operators of social engineering and a body of research on persuasion. If a relationship can be properly demonstrated, it is the author's thesis that the theories provided by social psychology on resisting persuasion can be theoretically generalized to the phenomenon of social engineering.

After a formal relationship between social engineering and persuasion is demonstrated, Chapter V then provides four prominent theories on the resistance of persuasion as novel applications for defending against social engineering. The theories of inoculation, forewarning, metacognition, and dispelling the illusion of invulnerability are discussed.

This document concludes with Chapter VI which remarks on the implications this research may have on the Air Force and other information security practitioners, the limitations of this research, and areas for future study.

II. LITERATURE REVIEW

"All of the firewalls and encryption in the world will never stop a gifted social engineer from rifling a corporate database or an irate employee form crashing a system. If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link—not operating systems, firewalls or encryption algorithms—but people"

–Kevin Mitnick (Thomas, 2008)

This chapter summarizes the literature that was reviewed in developing a starting point for answering the guiding research question. In order to achieve the goal of providing better protection to Air Force personnel from the types of information security breaches mentioned earlier, one must develop a comprehensive understanding of the common attack vectors and the derivation of those types of events. To accomplish these two tasks, an assessment was first conducted of the information security literature to help define the problem space and was followed by an examination of a few psychological constructs that may garner insight into the root causes of successful social engineering attempts.

2.1 Social Engineering Defined

The term "social engineering" as it is applied to information systems and computer hacking was popularized by Kevin Mitnick, the most wanted computer criminal in United States history at the time of his arrest in 1995 (Department of Justice, 1999).

Within this information systems application, social engineering can be broadly defined as the practice of using deceptive social and psychological methods on the human element in order to obtain protected information, obtain access, or influence behavior toward those objectives (Mitnick, 2003; Pipkin, 2000; Thornburgh, 2005).

In its basic form, social engineering is a suite of methods used to fool decision makers and is really nothing more than an updated form of frauds, confidence tricks, and other deceptions used by con-artists throughout history. Although the ideas behind social engineering in these forms have been documented for millennia, the onset of the cyber domain has allowed for the growth and complexity of the techniques to expand. It is for this reason that social engineering in its current state is an increasing threat to information security for organizations worldwide. To build a robust understanding of social engineering, a review of its most common process and techniques is essential.

2.2 The Social Engineering Cycle

To fully comprehend social engineering is to know it as a process, not as a single event. Malcolm Allen states that "each social engineering attack is unique, with the possibility that it might involve multiple phases and may even incorporate the use of other more traditional attack techniques to achieve the desired end result" (2007, pg 5). He goes on to say that any criminal act has a common pattern and such a pattern is evident with social engineering (pg 5). With the purpose of describing this pattern, Kevin Mitnick created the social engineering cycle which identifies 4 distinct phases: research, developing rapport and trust, exploiting trust, and utilizing information (2003), (Figure 2.1).

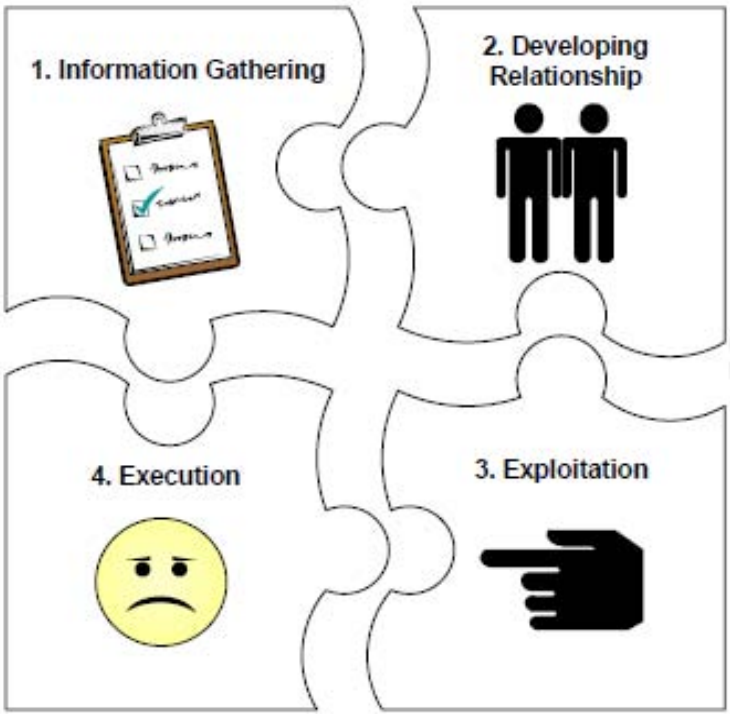

Figure 2.1 The Social Engineering Cycle (Allen, 2007)

In phase 1 of the social engineering cycle, various techniques are employed to gather information for the purpose of establishing credibility with a targeted individual or organization. Information often targeted includes organizational charts, personally identifiable information, open source information, etc. This information is gained through the use of both low-technology techniques such as simply making a request or dumpster diving and their high-technology analogs, web searches and hacking.

Developing rapport and trust, the second phase in the cycle occurs when the social engineer uses the insider information gained during the first phase to begin developing relationships with targeted individuals. To aid in the relationship building process, the engineer may use a variety of techniques such as name dropping, presenting false identities, or acting as, or on behalf of an authority.

In the third phase of the cycle, exploiting trust, the social engineer exploits the relationship to encourage the target to divulge information or perform actions that would not be granted without such an established relationship. Targeted information here includes such things as passwords, and includes unauthorized actions such as creating higher privileged accounts or granting access. If the information obtained in the third phase is only a piece needed to reach the final objective, the social engineer returns to an earlier phase to gain other needed information or actions. In this way, "a single cycle may produce only one piece of information that is then added to the research for the next cycle" (Thornburgh, 2005, p. 134).

The last phase of the cycle is utilizing information. This is the final execution of the attack using all that has been gained to compromise the information that was initially desired. It is important to note that during any one social engineering attempt, several different techniques may be used in conjunction and build upon one another. In addition, the targets are purposely randomized and changed often as not to raise suspicion. To this end, Pipkin writes "much social engineering will go unnoticed, since a hacker will ask one individual only a few specific questions and then move on. These Attacks will include numerous, inconsequential inquiries that add up to a great wealth of information" (2000, p. 216).

To simplify understanding, the individual techniques that are commonly applied in the social engineering cycle can be classified into two sub categories: human-mediated and technology-mediated. Human-mediated social engineering pertains to human-to-human interactions, where technology-mediated interactions pertain to those instances of social engineering where an electronic interface is used as an intermediary.

2.3 Human-mediated Social Engineering Techniques

Some of the most common human-mediated social engineering techniques that threaten information security of enterprises such as the Air Force include: pretexting, quid pro quo, and support staff. Pretexting is the use of an invented scenario to aid in the persuasion of a target to release information or perform unauthorized actions. This technique often involves prior research of the target to gather pieces of information that help establish legitimacy in the mind of the target. Pretexts often reported include the impersonation of other personnel in an organization in need of details, police officers or investigators "validating" information, or posing as authority figures such as company heads in a time critical situation asking for a password reset.

Quid pro quo is Latin for "this for that" and refers to a situation where information is given in exchange for a service. Common to this scenario, a social engineer calls targeted persons in an organization stating that they are a member of technical support trying to resolve some network problem. Once a target has been established, the engineer guides the victim through commands that give restricted access or an ability to launch malware.

A recent audit of IRS personnel conducted during a penetration testing exercise demonstrates the surprisingly high rate of success quid pro quo techniques can achieve. In a report for the Department of the Treasury, the Deputy Inspector states that "we made 102 telephone calls to IRS employees…and posed as computer support helpdesk representatives. Under this scenario, we asked for each employee's assistance to correct a computer problem and requested that the employee provide his or her username and

temporarily change his or her password to one we suggested. We were able to convince 61 of the 102 employees to comply with our requests" (2007, pg 2). The report goes on to state that only 8 of the 102 employees contacted security to validate that this was an official activity.

In the support staff scenario, a social engineer impersonates a member of some type of facility support staff such as the cleaning crew. In this role, a social engineer can physically access facility areas in an attempt to eavesdrop, shoulder surf, establish relationships, or remove pieces of information such as ID cards, confidential files, or other sensitive information from the trash. Gaining protected information from organizations by assembling seemingly disparate pieces of trash is known as dumpster diving. This practice is often used to gain organizational context and is used in the research phase for developing pretexts such as using discarded letterhead to recreate official looking correspondence. In addition to these activities, the support staff scenario has been used to place calls from the desks of company heads using an authoritative voice to encourage persuasiveness.

2.4 Technology-mediated Social Engineering Techniques

Just as is the case with human-mediated forms of social engineering, it is important to recognize and understand the common information security threats that have arisen in the digital era including: phishing, vishing, Trojan horses, and spam. Technology-mediated social engineering "utilizes the similarity between reality and digital communication to exploit cognitive biases in human decision-making. These biases prey on a human's proclivity to accept rewards, romance, charity, or other feelings

of sensitivity and emotion…since real issues and digital issues often coincide, humans are easily enticed into believing that what is false is real, and vice versa" (Thomas, 2008, p. 4).

Phishing is the use of digital communications, most often emails that appear to have come from a legitimate source such as a bank or credit card company requesting verification of sensitive information. These verification requests are usually done under the guise of circumventing some serious consequence. The term gets its name from a combination of the act of "fishing" for information, and a nod to the origins of computer hacking or "phreaking". These communications usually contain a link to a fraudulent web page with legitimate company logos or content, and requests information such as usernames, passwords, account numbers, pins, etc. as depicted in Figure 2.2.

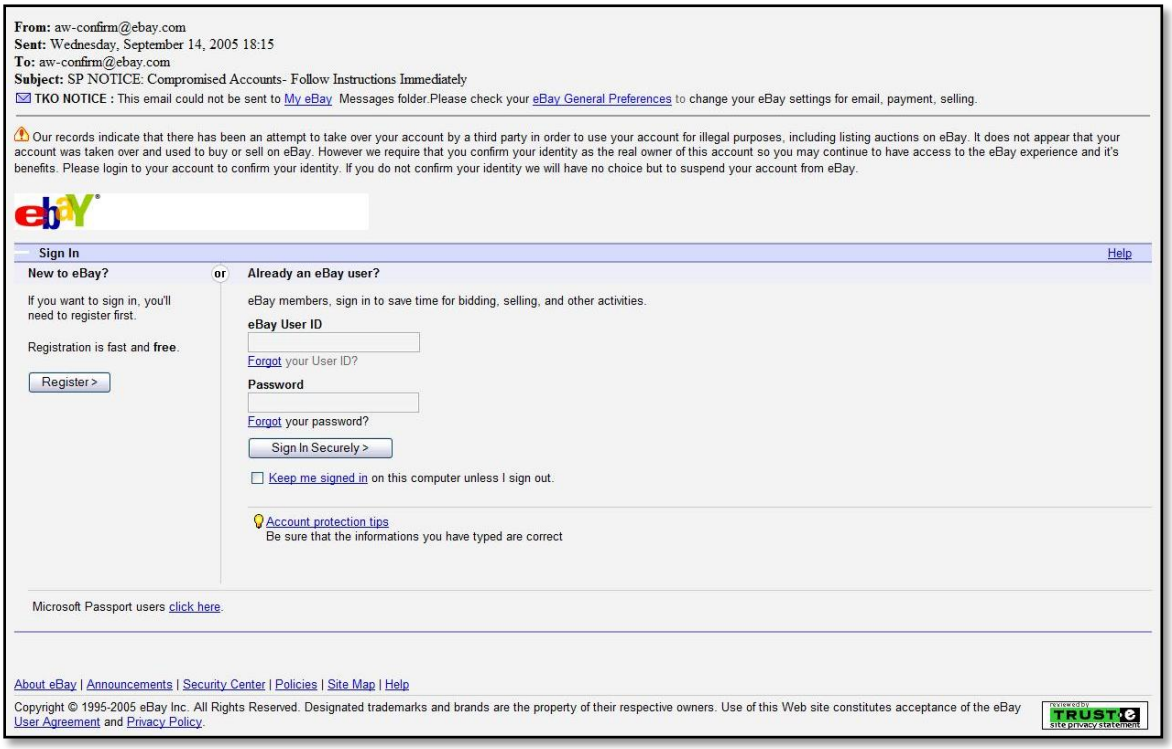

Figure 2.2 Ebay Phishing Scam (Ebay, 2011)

A highly targeted form of phishing in which the communication is only sent to a specific subset of victims such as within a company, government agency, or organization is known as spear phishing. This threat is especially common to military personnel who are often targeted for their level of security privilege and access to classified information.

Vishing is a combination of the terms voice and phishing wherein Voice over Internet Protocol (VoIP) technology is used to exploit trust in traditional landline telephone services that use Interactive Voice Response (IVR) systems. A victim or caller is directed to a rogue IVR system disguised as a real bank or credit card company IVR and is then prompted to verify information by entering account numbers, passwords, or PIN's. In some instances, victims have been transferred to the social engineer posing as a customer service agent in an attempt to reveal even more information through questioning.

The Trojan horse technique was so named after the Trojan War tale from Homer's Iliad, where gift giving was used by the Greeks to usher an attack on the Trojans. In the tale, a wooden horse was presented as a peace offering, but was actually a deception as it contained Greek soldiers and was used as gain them access inside the walls of Troy. As is the case in the story, computer-based Trojan horses come in the form of seemingly legitimate and desirable "gifts" such as software programs or a free download, but instead facilitate unauthorized access of the victim's computer system. After the Trojan horse malware has been installed on a victim's machine, the issuer may gain remote access to steal data or use the machine as part of a botnet for other nefarious purposes such as distributed denials of service.

A physical variation of the Trojan horse technique coined "baiting" or "road apples" occurs when a social engineer places a physical media device such as a USB thumb drive or CD infected with malware in a place where it will be found and relies on a victim's curiosity or goodwill to insert it into a computer system to gain access. This is the technique that was employed in the 2008 breach of CENTCOM networks, and suspected in the Stuxnet case mentioned earlier.

Spam refers to the broad use of electronic messaging systems such as email, instant messaging, mobile phone text messaging, and others to send unwanted messages with commercial content or malware to bulk address lists. The communications often prey on the human proclivity to accept friendships, gifts, prizes, pictures, or entertaining information along with the anonymity of the internet to entice users to download malicious code. It is important to note that although many of the human-mediated and technology mediated social engineering examples are discussed here, these techniques may take on numerous different forms and are purposely crafted to be unrecognizable as to what they actually are.

2.5 Tools of the Trade: The Social Engineering Toolkit

To demonstrate how the advent of the digital era has expanded the forms and complexity of social engineering techniques, one needs not look farther than the Social Engineering Toolkit (SET), (Figure 2.3). Developed by David Kennedy (aka ReL1K) for the penetration testing community social-engineer.org, SET is an application that combines several computer based social engineering tools in one package. Note the banner in Figure 2.3 stating "Welcome to the Social-Engineer Toolkit (SET), Your one

stop shop for all of your social-engineering needs".

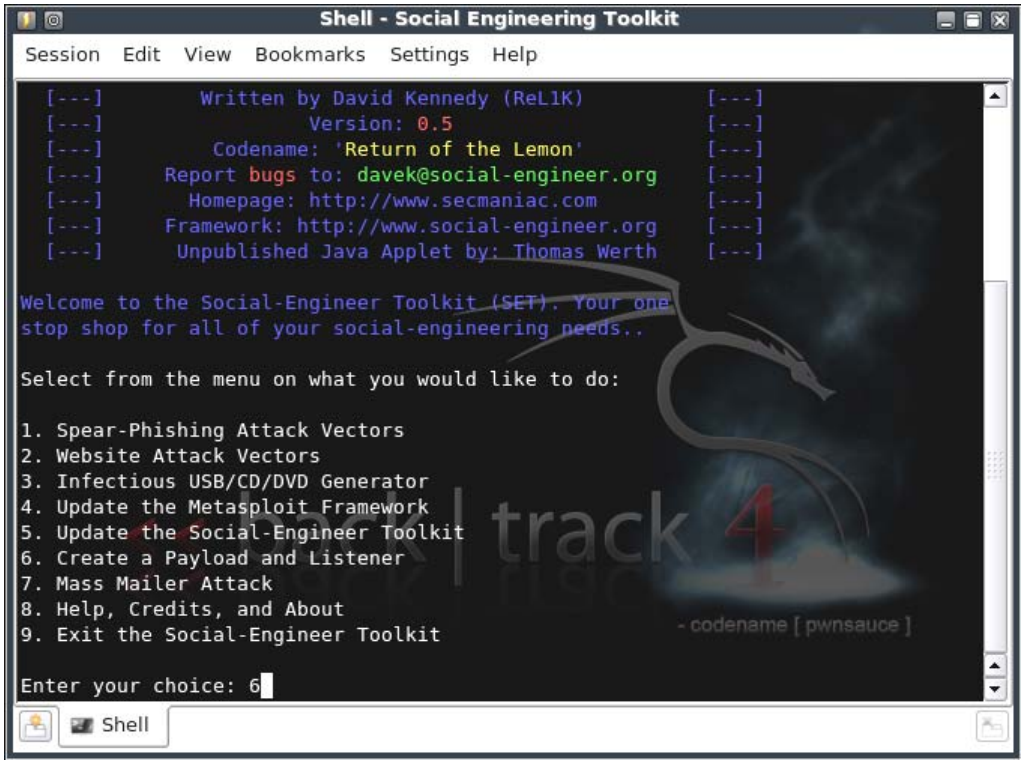

Figure 2.3 The Social Engineering Toolkit (SET, 2011)

The SET was specifically designed to perform sophisticated attacks against the human factor, and has quickly become a standard tool in penetration testing. Note that the attack vectors include many of those discussed in this report, and are about as easy to employ as making a selection from a menu. Other options available not depicted in Figure 2.3 include vectors such as Java Applet attacks, a web jacking attack, and an infectious media generator. Social engineering as a low-cost asymmetric attack methodology is no more evident than in the case of the SET.

Although it is the case that these information security attack vectors continue to rapidly grow and evolve along with the technological solution sets commonly used to

defend against them, the attributes that enable their success lie in human nature which remains relatively unchanged. Now that the more observable groundwork of identifying the process, common techniques, and tools of modern social engineering that threaten information security has been completed, the next step in answering the guiding research question is to develop a root-cause understanding about the psychological enablers of social engineering methods.

2.6 Routes of Persuasion

For any situation where a person intends to persuade another to do something, social psychology has identified two alternative routes that the persuader can employ, a central route and a peripheral route (Rush, 1999). "A central route to persuasion marshals systemic and logical arguments to stimulate a favorable response, prompting the listener or reader to think deeply and reach agreement. A peripheral route to persuasion, in contrast, relies on peripheral cues and mental shortcuts to bypass logical argument and seek to trigger acceptance without thinking deeply about the matter" (Rush, 1999, pg 3). Overwhelmingly, the peripheral route is the means by which social engineers try to persuade their targets and is the focus of this research.

A psychological exploitation commonly used by social engineers to make potential victims more susceptible to peripheral routes of persuasion is to elicit strong emotional responses such as excitement or fear. "Surges of strong emotion, like other forms of distraction, serve to interfere with a victim's capacity for logical thinking. This aids a social engineer in making false representations that exploit a peripheral route to persuasion" (Rush, 1999). A recent Microsoft Security Intelligence Report expands on

this idea and states that human emotions social engineers often prey on are: fear of loss or damage, desire for entertainment, acquisition or happiness, and trust in their work environment, institutions, friends and associates as shown in Figure 2.4 (2008, pp. 15-18).

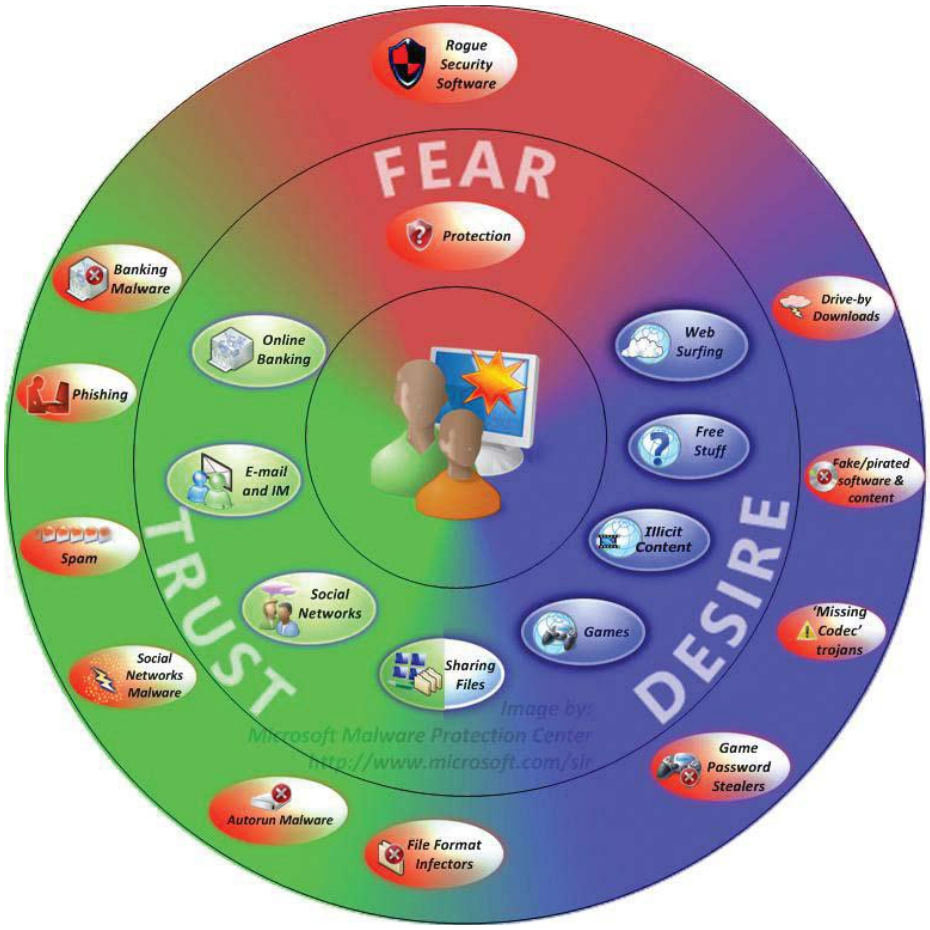

Figure 2.4 Common Targets of Social Engineering (Microsoft, 2008)

Key features to note in this depiction are the techniques such as those previously discussed (e.g., phishing, spam, Trojans), as well as other attacks associated with the fundamental human drives, emotions, and feelings which help to trigger the peripheral route to persuasion. Once this peripheral route of persuasion has been identified, one

wonders what it is specific to the human condition that allows for this vulnerability. Some psychologists theorize that humans have evolved with some of the same fixed-action patterns as our counterparts in the animal kingdom who display certain predetermined behaviors such as courting rituals.

2.7 Human Nature: Heuristic Thinking and Cognitive Biases

Traits inherent to human information processing include the phenomena of heuristics and cognitive biases, and lie at the heart of peripheral persuasion. Heuristics are nothing more than cognitive shortcuts and strategies based upon past experiences used by humans to establish quick solution sets to problems. Universal forms of heuristics in decision-making include: intuition, rules of thumb, educated guesses, and common sense. Although very efficient for day-to-day information processing, reliance on heuristics can cause gross errors in reasoning when applied improperly. When these cases arise and a heuristic is applied incorrectly in a systematic manner, it becomes a cognitive bias.

Naturally following then, cognitive biases are tendencies in reasoning which cause systematic errors in judgment. These bugs in the human hardware are frequent targets for social engineering tactics and include biases such as: the confirmation bias, a tendency to interpret information consistent with one's preconceptions; the exposure bias, in which people tend to like others (and other things) according to their familiarity; and the anchoring bias, in which a single trait or piece of information (like style of dress) is relied upon to make inferences about other qualities. "In fact, automatic, stereotyped behavior is prevalent in much of human action, because in many cases it is the most

efficient form of behaving, and in other cases it is simply necessary. You and I exist in an extraordinarily complicated stimulus environment; easily the most rapidly moving and complex that has ever existed on this planet. To deal with it, we *need* shortcuts" (Cialdini, 2006, pg 7).

These psychological principles demonstrate that influence through the distraction from systematic thinking is at the core of social engineering and is the fundamental skill engineers have for influencing targets. Heuristics and cognitive biases as routes to influence will persist regardless of technological development because they are traits inherent to the human condition. Further complicating this issue, Cialdini states "the evidence suggests that the ever-accelerating pace and informational crush of modern life will make this particular form of unthinking compliance more and more prevalent in the future. It will be increasingly important for the society, therefore, to understand the how and why of automatic influence" (2006, xiv). It is only through a thorough understanding of psychological principles and human traits such as these that will enable the development of effective mitigations to social engineering, *not through technological advancements*.

2.8 Psychological Foundations

While examining the underpinnings of social engineering through the lens of psychology, several seminal studies that exhibit pertinence to the techniques arise. Of particular interest is a long history of literature on compliance and obedience initiated by the work of Stanley Milgram, as well as several studies on authority and authority figures highlighted by Leonard Bickman.

In reaction to the atrocious behaviors displayed by Nazi concentration camp guards during WWII that seemingly conflicted with their personal conscience, Yale University psychologist Stanley Milgram set up a series of experiments to investigate the phenomenon of obedience. These experiments first conducted in the early 1960's and subsequently replicated many times, measured the willingness of participants to obey orders, even when those orders countered the belief systems held by participants (Milgram, 1973). These studies are especially insightful to the psychological enablers of social engineering in which people are seemingly encouraged against their will and established belief systems to divulge information or act inappropriately. This is especially evident in a hierarchically organized authority structure such as the military.

The first of the Milgram experiments was set up with a "teacher" (the Subject, or participant), a "learner" (the Actor, part of the investigative team), and an "Experimenter" (also part of the investigative team) (S, A, & E respectively in Figure 2.5). The participant was told that the experiment was investigating how punishment affects learning and memory, with electric shocks being used as a punishment. After observing the "learner" being hooked up to an electric shock generator and moving to an adjacent room (within earshot), the participant was then given a list of word pairs to read to the learner. The participant was then instructed to deliver electric shocks of 30 successively increasing voltages for incorrect or no answers given by the learner in response to the word pairs. Although electric shocks were not actually being delivered, the participant believed this to be true with the learner acting accordingly by screaming, pounding on the wall, pleas for stopping, and finally silence (Milgram, 1973).

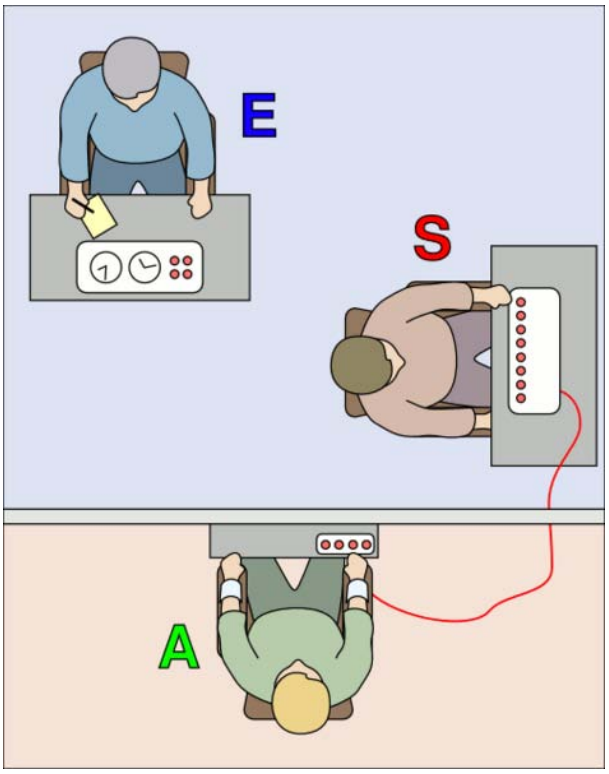

Figure 2.5 Milgram Experiment (Milgram, 2011)

After a few shocks were delivered, most participants questioned the experiment, showed signs of stress, and expressed a desire to stop. When this desire was verbally expressed, the "experimenter" (an authoritative scientist, dressed in a laboratory coat) responded with four successive responses that included: "please continue", "the experiment requires that you continue", "it is absolutely essential that you continue", and lastly "you have no other choice, you must go on". The experiment was concluded when either the participant expressed a desire to stop after all four commands were given or when the maximum punishment of 450 volts was delivered three successive times (Milgram, 1973).

The published results of the study indicated that 65% of participants delivered all 30 shocks ending with the maximum 450 volt shock in which the learner was silent (and

presumed unconscious or dead). "The results surprised everyone associated with the project, Milgram included. In fact, before the study began, a group of 39 psychiatrists predicted that only about one person in a thousand would be willing to continue to the end. No one, then, was prepared for the behavior patterns that the experiment actually produced" (Cialdini, 2006, pg 211). These experiments on obedience shed some light as to why the techniques of social engineering which would seem to require a lack of will or exaggerated gullibility on the part of its victims enjoy such a high rate of success.

In another study, "The social power of a uniform" published by psychologist Leonard Bickman, a research assistant in either plain clothes, or a police-style uniform commanded random pedestrians on a city street to either pick up a paper bag, give bus fare to another person, or step back from a bus stop. In the plain clothes condition, researchers found that only 42% of citizens complied with the research assistant versus a 92% rate of compliance in the police uniform condition (Bickman, 1974).

These studies highlight areas of experimental psychology that have demonstrated the powerful social significance commitment, authority figures and appearance have, and how they may be used to manipulate others. Individuals seek clues about others from their appearance such as dress to make mental shortcuts in identifying occupation, authority, legitimacy, group membership, status, etc. This is especially evident within military organizations that condition their personnel to obey orders based on authoritative rank. It is exactly these shortcuts that social engineers leverage to exploit their targets.

2.9 Two Frameworks: Mitnick & Cialdini

In the process of reviewing the literature from the information security and psychology arenas, two prominent frameworks for understanding the psychological enablers of social engineering emerged beyond what has been covered here. One of these frameworks comes from the convicted social engineer turned security consultant Kevin Mitnick himself. Although lacking formal scientific or academic training, Mitnick's experiences and status as a subject matter expert make him uniquely qualified to make invaluable observations of these phenomena.

In contrast, the other useful framework that emerged comes from best-selling author and noted social psychologist Dr. Robert Cialdini. Dr. Cialdini is a formally educated PhD working as a professor of psychology and marketing at Arizona State University. While these two individuals come from very different backgrounds, they have each created constructs for understanding human nature that the author believes to be very closely related and could provide an avenue for novel information security research. To initially call attention to this linkage which is detailed in Chapter IV, Mitnick describes social engineering as "the art of influence and persuasion" (2003), where Cialdini describes his framework on persuasion as "the science of influence" (2006).

This chapter provided the foundation upon which the rest of this research rests. The constructs introduced here will be revisited and made more pertinent to the thesis with a qualitative analysis in chapter IV. To reach that step, the next chapter outlines the methodology employed to make that analysis.

III. RESEARCH METHOD

"It may be that we are puppets-puppets controlled by the strings of society. But at least we are puppets with perception, with awareness. And perhaps our awareness is the first step to our liberation."

–Stanley Milgram

The purpose of this chapter is to document the methodology employed during the course of this research. It describes the evolution of ideas throughout the research process, introduces the methods that were employed, and provides the justifications for why these methods were chosen. In particular, the research process for this work consisted of four distinct phases. It began with a survey of literature from the information security field, followed with literature review of social psychology, a qualitative analysis performed on two of the seminal works from these domains, and an exploratory analysis of established theories on the resistance of persuasion applied to the threat of social engineering.

3.1 Research Questions

The initial inspiration behind this research was the simple question "How can the Air Force protect its personnel from the increasing information security threat of social engineering attempts such as in the case of the 2008 CENTCOM breach?" From this initial research question, several other investigative questions were developed and together became the guiding framework for this effort. These investigative questions

include: “Is there a relationship between the deceptive techniques of social engineering as described in the information security community and the body of research on persuasion found in the social psychology community? If a relationship exists, “What is the nature of the relationship?” Also, “Can this relationship be formally demonstrated?” If so, “Does the body of research on persuasion provide any insight on how people can be protected from techniques of social engineering?” And lastly, “What are some testable hypotheses that can be formulated base upon the establishment of this relationship?”

3.2 Approach

To begin to formulate an answer to the aforementioned primary research question and investigative questions, a thorough understanding of social engineering tactics and their underlying enabling features would need to be established. To build this understanding of social engineering, the first step was to perform a review of the relevant literature.

Because of the novelty of the social engineering phenomenon, one quickly finds that there is not a great deal of formalized scientific research available for review on the problem. This finding had two distinct consequences on the course of this research. The first was that due to the lack of empirical research on social engineering, the importance of anecdotal accounts from subject matter experts and from the information security trade literature became paramount. Second, broadening the scope of search to explore possible interrelated domains proved to be indispensable for developing a complete understanding of the issues at play. Due to the author’s formal training and familiarity, an exploration

of the social psychology literature for theories that were potentially applicable to the issue of social engineering followed.

During an extensive review of these two domains, several themes began to emerge. The first was that the underpinnings of social engineering techniques may be able to be captured into a relatively small set of core concepts. The second was that a relationship between these core concepts and a model universally accepted among social psychologists for understanding the phenomenon of persuasion may exist. Lastly, the survey of social psychology research turned up several established theories for building resistance to persuasion. After these themes emerged, the next logical step would be to formalize this relationship so that these theories on the resistance to persuasion could be examined for their application to the social engineering problem.

3.3 Qualitative Analysis

To move beyond this informal observation toward establishing a formal link between the core components of social engineering and established concepts of human persuasion, a validated methodology was needed. Because of the time and resource constraints particular to this effort, an inductive framework that supports theory building for other more resource intensive analyses would be optimal. Thus, a qualitative analysis of the information captured in the literature review became the general strategy for establishing this link. This also helped to scope the outcome objectives of the current effort to the creation of hypotheses for other more resource intensive analyses such as quantitative laboratory experimentation.

3.4 The General Inductive Approach

The qualitative analysis as a validated research method to conduct investigations of concepts such as those found in this research is well documented. "Many of these are associated with specific approaches or traditions, such as grounded theory, phenomenology, discourse analysis, and narrative analysis. However, some analytic approaches are generic and are not labeled within one of the specific traditions of qualitative research" (Thomas, 2006, pg 237). As the objectives of this research effort did not necessarily lend themselves to one of the more traditional qualitative analysis approaches, a general inductive approach was adopted (Figure 3.1).

Comparison of Qualitative Analysis Approaches

	General Inductive Approach	Grounded Theory	Discourse Analysis	Phenomenology
Analytic strategies and questions	What are the core meanings evident in the text, relevant to evaluation or research objectives?	To generate or discover theory using open and axial coding and theoretical sampling	Concerned with talk and texts as social practices and their rhetorical or argumentative organization	Seeks to uncover the meaning that lives within experience and to convey felt understanding in words
Outcome of analysis	Themes or categories most relevant to research objectives identified	A theory that includes themes or categories	Multiple meanings of language and text identified and described	A description of lived experiences
Presentation of findings	Description of most important themes	Description of theory that includes core themes	Descriptive account of multiple meanings in text	A coherent story or narrative about the experience

Figure 3.1 Traditional Qualitative Analysis Approaches (Thomas, 2006)

Of note in Figure 3.1, the general inductive approach aided this effort in identifying core meanings of social engineering behavior and of the themes most relevant to the research objective of discovering emerging hypotheses for defending against social

engineering. This was possible by providing a less prescriptive method than other closely related traditional qualitative analyses such as grounded theory or phenomenology. To this end, Thomas puts forth that "the general inductive approach provides an easily used and systematic set of procedures for analyzing qualitative data that can produce reliable and valid findings" (2006, pg 237).

In the employment of the general inductive analysis approach, Thomas identifies three purposes:

1. To condense extensive and varied raw text data into a brief, summary format;
2. To establish clear links between the research objectives and the summary findings derived from the raw data and to ensure that these links are both transparent (able to be demonstrated to others) and defensible (justifiable given the objectives of the research; and
3. To develop a model or theory about the underlying structure or experiences or processes that are evident in the text data (2006, pg 238).

To accomplish these purposes, the general inductive approach makes use of the same inductive coding process as other related qualitative approaches. This process consists of five steps which are depicted below in Figure 3.2. Following this figure then, the steps are to:

1. Conduct an initial survey of the literature.
2. Identify specific segments of the literature related to the research objectives.
3. Construct categories of patterned behavior from those segments identified.
4. Reduce categorical redundancy.
5. Develop a model that contains the significant categories to the objectives.

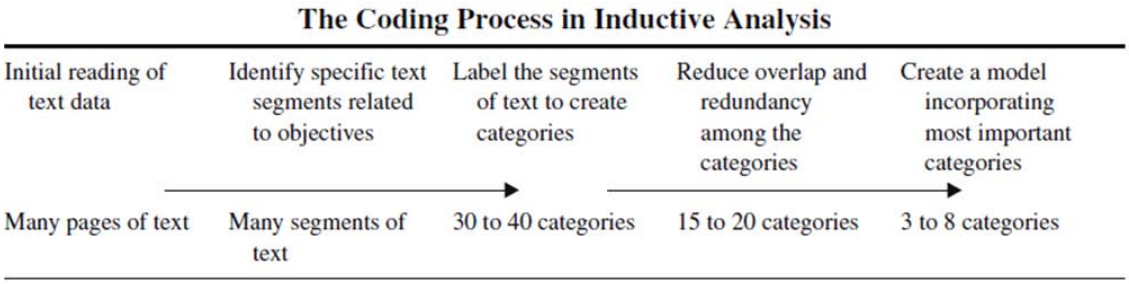

Figure 3.2 Inductive Analysis Coding Process (Thomas, 2006)

3.5 Research Objectives

The next chapter provides a detailed description of the qualitative analysis conducted. In conducting an inductive analysis, Thomas specifies that "the inductive approach is a systematic procedure for analyzing qualitative data in which the analysis is guided by specific evaluation objectives" (2006). As such, it is important to explicitly state those objectives here.

The three main objectives of the analysis conducted in Chapter IV are to identify segments of the literature that provide unique understanding about the psychological underpinnings of social engineering, formally demonstrate a relationship between social engineering techniques and the principles of persuasion, and lastly to create a model that accurately represents the psychological enablers of social engineering. If these objectives are met, it will provide the foundation for developing testable hypotheses for follow on studies that improve our understanding of how to defend against social engineering**.**

IV. ANALYSIS

It is easier to resist at the beginning than at the end.

–Leonardo Da Vinci

This chapter presents the qualitative analysis that was performed on the aforementioned frameworks of social engineering and persuasion that emerged during the literature review. Before this analysis is detailed it is necessary to explicitly state the rationale behind this exercise beyond what has been provided so far. That rationale is given by a frame of reference for the analysis, the grounds for inclusion, and the author's thesis.

4.1 Rationale

To give context to this analysis a common frame of reference needs to be established, and that frame of reference is the phenomenon of compliance. The psychological techniques that most effectively influence one person to acquiesce to another are the common threads that run through these two frameworks. Although emerging from different domains, and employed for different objectives, the essential outcome shared between them is getting a person to say "yes" to a request.

From the vantage of Kevin Mitnick, and that of a social engineer, the objective is to nefariously obtain compliance from a targeted victim. In the same sense, Cialdini's framework on persuasion comes in part from research he did on "compliance practitioners": advertisers, public relations personnel, and fund raising agencies looking for that same "yes" response (2006). An informal observation of these two models

reveals that Mitnick's social engineer would easily qualify as one of Cialdini's "compliance practitioners".

The grounds for including these two specific frameworks in an analysis reside in the fact that both are put forth by recognized subject matter experts in their fields of practice, are frequently cited, and are considered seminal works within their respective domains. In addition, both are presented as categorical models for understanding human behavior that together could provide an avenue for novel information security research. Specific to that relationship, it is the author's thesis is that these two frameworks describe the same phenomena, and in that regard they corroborate and extend each other.

4.2 The Coding Process

In review from Chapter III, the coding process of the inductive analysis consists of five steps which were depicted in Figure 3.2. Following that figure, but specific to this research effort then, the steps of this analysis were to:

1. Conduct an initial survey of the phenomenon of social engineering through the lens of information security and social psychology.
2. Identify specific segments of the literature related to the objective of providing understanding about the psychological underpinnings of social engineering.
3. Construct categories of patterned behavior from those segments identified.
4. Reduce categorical redundancy.
5. Develop a framework for developing hypotheses about the novel application of social psychology theory to social engineering.

As steps 1 and 2 of this process were captured by the efforts documented in the literature review, the remaining three steps are the focus of this chapter. Logically following, the next segment will present the categories of patterned behavior put forth by Mitnick & Cialdini. Subsequently, a segment providing detailed descriptions of those categories that demonstrates their correlations while reducing categorical redundancy is presented. Lastly, the output of the coding process will be revealed in a new framework that contains the most important 3-8 categories as prescribed by Thomas.

4.3 The Categories

In the course of reviewing the information security trade literature for information on social engineering, one will undoubtedly be led to Kevin Mitnick. The most sought after computer criminal at the time of his arrest in 1995, Mitnick pleaded guilty to four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting a wire communication (USDoJ, 1999). According to a U.S. Attorney's Office press release "Mitnick admitted that he broke into a number of computer systems and stole proprietary software belonging to Motorola, Novell, Fujitsu Siemens, Sun Microsystems and other companies…he admitted using a number of tools to commit his crimes, including social engineering…and admitted that he stole E-mails, monitored computer systems and impersonated employees of victim companies" (USDoJ, 1999).

After Mitnick's computer hacking exploits landed him in incarceration for these various computer and fraud related crimes, he served 46 months in federal prison and now serves as a security consultant providing his subject matter expertise on social engineering. Aside from his consulting work, Mitnick has published two books that

capture his expert knowledge of social engineering, *The Art of Deception: Controlling the Human Element of Security*, and *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. In the latter text, Mitnick puts forth a framework of psychological insights for understanding the most common tactics of social engineers which is summarized in Figure 4.1 below.

Category	Description
Trappings of Role	The tendency to use a few characteristics of others to infer other associated role attributes and act on those assumptions
Credibility	An inclination to infer global credibility or trustworthiness based upon an anchor event or validating trusted information
Altercasting	People will act in accordance to certain roles and relationships that have been established
Distracting from Systematic Thinking	Events that elicit strong affect influence people to use a heuristic rather than systematic information processing mode
Momentum of Compliance	A tendency to act in accordance to previous behaviors and commitments made
The Desire to Help	The social inclination of humans to act in helpful ways
Attribution	The tendency to explain others' behavior based upon a single observation or piece of information
Liking	The tendency to like others based upon shared characteristics, the use of flattery, or physical attractiveness and granting requests accordingly
Fear	Events that elicit a fear response influence people to use heuristic information processing and is a strong behavioral motivator
Reactance	The psychological reaction of desire in response to the loss freedoms, property, or in the case of scarce resources

Figure 4.1 Mitnick's Psychological Insights of Social Engineering (2005)

Particular attributes to note in this figure are the inclusion of ten categories that aim to capture the psychological underpinnings of social engineering in the left column and their associated descriptions to the right. Describing this framework in the book,

social psychologist Brad Sagarin is quoted as saying "There's nothing magic about social engineering. The social engineer employs the same persuasive techniques the rest of us use every day. We take on roles. We try to build credibility. We call in reciprocal obligations. But unlike most of us, the social engineer applies these techniques in a manipulative, deceptive, highly unethical manner, often to devastating effect" (2005, pg 232).

Alluding to a similar idea, noted social psychologist and best-selling author Robert Cialdini postulates that **"**although there are thousands of different tactics that compliance practitioners employ…the majority fall within six basic categories. Each of these categories is governed by a fundamental psychological principle that directs human behavior and, in so doing, gives the tactics their power" (2006, xii). These principles that rely on the aforementioned peripheral route of persuasion and cognitive biases include: Authority, Commitment & Consistency, Liking, Reciprocation, Scarcity & Social Proof, and are summarized in Figure 4.2 below.

Category	Description
Authority	A strong psychological bias for being responsive to assertions of authority
Commitment & Consistency	Personal and interpersonal pressure to behave in a manner consistent with previous commitments or behaviors
Liking	An inclination to help others according to familiarity, likeability or those that share similar social characteristics
Reciprocation	A tendency to feel an obligation to repay in kind, gifts or acts of kindness
Scarcity	The tendency to be responsive toward indications that objects or opportunities are in short supply
Social Proof	A tendency to view behavior in social situations as acceptable to the degree that others behave in the same manner

Figure 4.2 Cialdini's Principles of Persuasion (2006)

Cialdini goes on to state in his work; *Influence: The Psychology of Persuasion* that "each principle is examined as to its ability to produce a distinct kind of automatic, mindless compliance from people, that is, a willingness to say yes without thinking first (2006, xiv). At a first glance one can see the casual similarities between the two frameworks, even to the extent that the two share a categorical descriptor: Liking. There are some differences that include Cialdini's framework being based upon data sets composed of observations, interviews, and case studies whereas Mitnick's framework is based upon personal accounts, testimonials, and subject matter expert interviews. In this way, the author believes these two extend rather than complicate each other. To show this, a more in depth description of these categories, their relationships, and a reduction of their redundancies will follow as prescribed by the general inductive approach.

4.4 A Closer Look

By reviewing Figures 4.1 and 4.2, one can see that Mitnick's framework contains ten categories, and Cialdini's contains six. Together these frameworks contain sixteen categories that contain a degree of overlap. Following Thomas's coding process from Figure 3.2; the next step in the coding process is to reduce those elements to achieve 3-8 significant categories for modeling the underlying psychological enablers of social engineering.

To simplify the task of reducing categorical redundancy it was useful to employ a lens comparison technique. In this technique, one subject of interest is used as a reference point (or lens) for analyzing another. Specific to this analysis, Cialdini's

framework contains a smaller number of categories and thus was used as the lens for viewing the categories in Mitnick's framework.

The first of Cialdini's six principles states that people tend to have a strong bias for being responsive to assertions of authority. As established earlier with Milgram and Bickman's experiments, several studies have demonstrated an extreme willingness of adults to comply with the command of an authority, even if that authority figure is not physically present. Looking back to Mitnick's framework, this principle of authority seems to be captured as one subset under the broader category of Trappings of Role.

A trapping of role occurs when a social engineer exhibits a few characteristics of the role they are trying to impersonate in an attempt to get their victims to infer other related characteristics. Common characteristics displayed include style of dress, using industry jargon, name dropping, and include the impersonation of authority figures such as company heads. Psychological literature has demonstrated that people often use a few characteristics as anchors about which other associated character traits are assumed. Put another way, this is our strong propensity for using stereotypes. After analyzing these two categorical descriptors in this context, one can see that the authority principle is a subset of trappings of role and can be reduced down to one category for a new model. Thus, **Authority & Trappings of Role = Trappings of Role**.

The second of Cialdini's principals states that society places value on consistency of behavior and commitment to prior statements made. Once a person acts according to certain rules or makes a promise, they will encounter personal and societal pressures to behave consistently with those commitments. This happens because falling outside of these social norms would deem a person untrustworthy and undesirable.

Social engineers take advantage of this phenomenon by receiving a promise of help for several small favors and then going on to make larger requests for privileged information that would not be granted independently of the initial commitment. This is the technique Mitnick termed "momentum of compliance". Therefore, the technique of momentum of compliance can be understood as a subset of the psychological construct of commitment and consistency and reduces the redundancy of these categories. For the development of a new model then, **Commitment & Consistency, & Momentum of Compliance = Commitment & Consistency**.

Liking and similarity is the third principle of influence put forth by Cialdini. This principle states that we have a bias toward granting privilege to individuals that we are similar to or like. It is a human tendency to like characteristics resembling our own such as style of dress, occupation, social status, or personal interests and provides the social engineer with an access point for compliance.

By exploiting influences on liking such as similarity, using compliments, association effects, appealing to ego, and constant contact, the social engineer provides a strong incentive for their target to adopt a mental shortcut for perceiving him or her more favorably and thus dealing with their requests. Even a shallow analysis shows that Cialdini's principle of liking and Mitnick's liking category overlap by describing the same phenomenon. Accordingly, **Liking & Liking = Liking** for the new model.

Reciprocation, the fourth principle of influence asserts that people feel a strong obligation to repay other gestures of kindness with favors, even if that favor is significantly costlier that the original gesture. This well recognized social norm is often utilized by the social engineer who offers small favors or gifts before requesting targeted

information. In addition to gift giving, the reciprocation rule can be evoked by reciprocal concession in which a social engineer creates the perception that a concession has been made. In this "rejection then retreat" trick an attacker makes an initial egregious request and then accepts rejection of the initial request for a lesser but still targeted concession.

Although Mitnick describes paying compliments as part of his liking category, it doesn't capture the construct that Cialdini is describing here. As such, there is no analog to reciprocation in the Mitnick categories and we will keep Cialdini's **Reciprocation** as a unique category in the formation of a new model.

Cialdini's scarcity principle states that individuals are very responsive toward indications that objects or opportunities are in short supply or only available for a short time. In this cognitive bias, people tend to place an inordinate amount of value on the item or opportunity perceived to be scarce. In addition, renowned psychologist Jack Brehm's seminal theory of psychological reactance shows that this desire increases when the perception that others are competing for an item of short supply. Mitnick states that social engineers take advantage of this phenomenon by cultivating scenarios of short time supply or the loss of data to influence targets people into making decision based upon heuristic thinking rather than critical thinking.

Upon closer inspection, one can see that Cialdini's scarcity principle and Mitnick's reactance both operate by evoking heuristic information processing by using a fear response. In addition, Mitnick describes this overarching construct of influencing victims away from systematic information processing to one of heuristic processing as "Distraction from Systematic Thought". Therefore, in the sake of reducing this

redundancy for a new model **Scarcity & Reactance = Distraction from Systematic Thought**.

The last of Cialdini's principles states that people tend to view behavior in a given social situation as acceptable to the degree that others behave in the same manner. This principle termed social proof is a mental shortcut in which people determine appropriate behavior for any social setting based upon the behavior of others in their vicinity. Several well known anecdotes that evidence this phenomenon include the Jonestown mass suicide, as well as the highly publicized Kitty Genovese murder in which social proof was at play through dispersion of responsibility. Social engineers often prey on this social proof heuristic to prompt targets into taking actions against their own self interests. As was the case with the principle of reciprocation, there does not seem to be any analogous categories in Mitnick's framework. Thus Cialdini provides a unique descriptor in **Social Proof** and is added to the new model.

To this point all of Cialdini's principals have been captured leaving a few more categories from Mitnick that seem to provide unique insights of their own. Two of these categories include credibility and attribution. Mitnick describes the credibility tactic as a set of techniques used build the credibility of the engineer in the mind of the victim, and is the first step in most attacks. The techniques include using communication consistent with persons of trust such as an IT specialist encouraging a user to never disclose a password, predicting a network outage then causing that outage, or helping to fix such a caused problem.

Similarly, this framework contains the construct of attribution. Mitnick states that "Attribution refers to the way people explain their own behavior and that of others. A

goal of the social engineer is to have the target attribute certain characteristics to him or her, such as expertise, trustworthiness, or credibility" (2005, pg 236). For example, to evoke the global characteristic of trust, an engineer might act as if they are trying to find the rightful owner of money that was never lost. By inspecting Mitnick's own description of attribution, it can be noted that credibility is contained in the description. Therefore, credibility can be captured under attribution and **Credibility & Attribution = Attribution** for the new model.

The last two unexplored categories of the Mitnick framework are the desire to help and altercasting. The desire to help describes the well known attribute of humans as social beings and having an inclination to be supportive. Helping others has been shown to provide the helper with a feeling of empowerment, positive affect, and can make them feel good about themselves. By providing an outlet for people to be helpful, an engineer can take advantage of this inclination.

Much in the same way, altercasting describes a tactic wherein the social engineer persuades the victim to adopt a role beneficial to the engineer. Mitnick states that "In its most common form, the social engineer puts his or her target into the role of helper…people are likely to accept roles that are positive and that make them feel good" (2005, pg 234). By operating under the assumption of a person in need, the social engineer is evoking the desire to help as well as altercasting. As this is the common operator by which altercasting is employed in social engineering, the two categories can be collapsed into one such that **The Desire to Help & Altercasting = Altercasting** for a new model.

4.5 A New Model

Now that the tasks of formalizing a relationship between these frameworks and reducing categorical redundancy have been accomplished, last step in the coding process is to construct a new model for developing testable hypotheses about the novel application of social psychology theory to social engineering. By taking the outputs of the previous segment and using those as inputs for a new framework, we arrive at the model which is depicted in Figure 4.3. Note that the previous sixteen categories provided by Mitnick and Cialdini have been correlated and reduced into an eight component model that provides a more accurate platform for applying social psychology constructs to social engineering.

Category	Previous Categories	Description
Trappings of Role	Authority & Trappings of Role	The tendency to use a few characteristics of others to infer other associated role attributes and act on those assumptions
Commitment and Consistency	Momentum of Compliance & Commitment and Consistency	Personal and interpersonal pressure to behave in a manner consistent with previous commitments or behaviors
Liking	Liking & Liking	An inclination to help others according to familiarity, likeability or those that share similar social characteristics
Reciprocation	Reciprocation	A tendency to feel an obligation to repay in kind, gifts or acts of kindness
Distracting from Systematic Thought	Scarcity, Reactance & Distracting from Systematic Thought	Events that elicit strong affect influence people to use a heuristic rather than systematic information processing mode
Social Proof	Social Proof	A tendency to view behavior in social situations as acceptable to the degree that others behave in the same manner
Attribution	Credibility & Attribution	The tendency to explain others behavior based upon a single observation or piece of information
Altercasting	Desire to Help & Altercasting	People will act in accordance to certain roles and relationships that have been established

Figure 4.3 Psychological Enablers of Social Engineering

Looking back, the three main objectives of this analysis were to; identify segments of the literature that provide unique understanding about the psychological underpinnings of social engineering and present categories of patterned behavior from those segments, formally demonstrate a relationship between social engineering techniques and the principles of persuasion, and lastly to create a model that accurately represents the psychological enablers of social engineering. As those objectives were met, it provides the way forward for hypothesis development. In the next Chapter, a set

of theories developed by social psychologists for building resistance to persuasive attempts are presented as they can now be theoretically extended to the threat of social engineering.

V. DISCUSSION

Some people think technology has the answers

–Kevin Mitnick

Now that a formal relationship has been demonstrated between the enablers of social engineering and the principles of persuasion as defined by social psychology, some substantiated inferences between them can be made. Specifically, theories from social psychology pertaining to the resistance of persuasion can now be justifiably generalized for the application of defending against social engineering. In this chapter, four such validated theories will be presented as potential mitigations to this threat. But before detailing those theories it is prudent to reiterate why these novel approaches are needed. To demonstrate this, two segments are presented that address why the common mitigation approaches of technology patches and policy changes have continued to be inadequate solutions to the problem.

5.1 The Inadequate Technological Solution Set

While the majorities in the commercial and government sectors agree that human-based threats to information security are a growing problem, there are many security consultants, in addition to an entire cottage industry that continue to push technology-based solutions. This is evidenced by the countless technological security mechanisms that have been created and implemented including; firewalls, filters, password control mechanisms, intrusion detection, anti-virus software, anti-spyware, and the like. Demonstrated monetarily, it has been estimated that the commercial email security

market alone has grown from $3.3 billion in 2007, to $16.5 billion in 2010 in an effort to combat the rise in spam, viruses and other email threats (Crain, 2010).

Despite the rise of technological stop-gaps such as these, the continued demonstrations of vulnerability by military organizations dictate that a new approach is needed. Short term patches to constantly evolving technologies quickly become obsolete. Referring to these technology-based social engineering mitigations, Pipkin emphasizes "Technical solutions solve technical problems. People problems require personal solutions" (2000, p. 78). To address this problem from a long term perspective then, a human-centric solution set is needed.

5.2 The Policy Approach

From a defense sector perspective, the current position for defending Department of Defense (DoD) information against social engineering attacks seems to be a never ending cycle of information restriction policies reactionary in nature to the security incidents of recent history. This is evidenced by the recent DoD wide policies prohibiting the use of removable media on network computers following the 2008 USCENTCOM breach, and the banning of write privileges on all classified systems after the WikiLeaks incident.

These policies have since had the unintended consequence of restricting information sharing efficiencies (Nakashima, 2010). As AFDD 2-5 Information Operations states that "decision superiority is about improving our capability to observe, orient, decide, and act (OODA loop) faster and more effectively than the adversary" (2005, vii), these policies seem to be in conflict with stated operational goals. If the Air

Force wants to bolster information security without stifling the flow of information, a proactive human-centered approach is required.

This study has already demonstrated that a substantial body of research as well as the efforts of compliance practitioners such as advertisers, marketers, and social engineers has been devoted to understanding how to make individuals receptive to persuasive attempts. Even though this information provides a great deal of insight to the issue at hand, it is the converse of this that is needed to address the guiding research question. That is, what information exists that is devoted to understanding how to make individuals resistant to attempts at persuasion?

Although the majority of work in social psychology on persuasion has been dedicated to the former task, there are some clear lines of research devoted to the latter. Specifically, the psychological theories of inoculation, forewarning, metacognition, and dispelling the illusion of invulnerability address the resistance of persuasion and can be theoretically applied to the issue of social engineering now that a formal link is in place.

5.3 Inoculation

The first of these four theories to emerge from the literature in 1961 is McGuire's theory of Inoculation. Just as Stanley Milgram's work was a response to observations of compliance in WWII, William McGuire's work on inducing resistance to persuasion was a response to events observed in the Korean War. During the conflict, several American prisoners of war had apparently succumbed to the influence of their enemies when they renounced the U.S. effort and opted to remain in with their captors. "Congressional hearings following the war raised alarm about the seeming effectiveness of North Korean

"brainwashing" techniques. How might such brainwashing be prevented? This question was the catalyst for McGuire's interest in ways to instill resistance to propaganda and other forms of influence" (Pfau & Szabo, 2003, pg 266).

To answer this question, McGuire derived a theory based upon an analogy to the practice of inoculation against biological disease. In such a medical inoculation, a person is exposed to a weakened form of a virus, weak enough that the body can fight it off, but strong enough to produce a significant response from the immune system. That response includes the production of antibodies which can fight off a stronger infection later. Much in the same way, McGuire's theory of cognitive inoculation states that resistance to persuasive messages can be obtained by exposing people to weak arguments that counter their beliefs and giving them a chance to refute those arguments. This in turn creates stronger counterarguments and confers resistance to stronger attempts at persuasion later on (McGuire, 1961).

To test his theory, McGuire conducted a series of experiments, the first of which tested inoculation on what McGuire termed "cultural truisms". "Cultural truisms are beliefs that are so widely shared within the person's social milieu that he would not have heard them attacked" (McGuire, 1964, pg 201). This was done to obtain an untainted set of beliefs that are not argued over often such as "It's a good idea to brush your teeth", "Mental illness is not contagious", and "The effects of penicillin have been of great benefit to mankind". After validating the idea that attitudes and beliefs could be strengthened by prior exposure to weakened arguments against cultural truisms, McGuire and others extended the theory to more useful belief sets including advertising, politics, public health, and the like.

As the theory stands today, two key elements are regarded as necessary for successful inoculation; threat and refutational preemption. The first of these, threat, is an indication that specific existing attitudes are vulnerable and may be challenged. "Thus, the threat serves as the motivational trigger in the inoculation model" (Pfau & Szabo, 2003, pg 267). On the other hand, refutational preemption is the process of demonstrating opposing arguments as well as the evidence and arguments to refute them. "Threat motivates the individual to bolster his or her attitudes; refutational preemption offers specific content that can be used to protect and defend ones attitudes" (Pfau & Szabo, 2003, pg 267).

Following this theory then, it is hypothesized that the successful application of cognitive inoculation in a training program built to bolster resistance to social engineering would require the same threat and refutational preemption elements. The threat element could come in the form of testing personnel about their beliefs of policy under different pretexts common to social engineering during regular training, compliance testing, or during penetration tests. Refutational preemption could then be provided by demonstrating counterarguments and anecdotal evidence in support of that policy to personnel. In addition, McGuire & Papageorgis state that "the refutational defense is effective in producing resistance to subsequent attacks even when these attacks involve counterarguments other than those refuted in the defense" (1962, pg 25). In this way, it is the author's belief that applying the tenets of inoculation theory to a social engineering training program could provide a robust approach to defending Air Force personnel from this threat.

5.4 Forewarning

In addition to inoculation, McGuire & Papageorgis demonstrated the effectiveness of forewarning in developing resistance to persuasion. "This manipulation involves announcing to the person in advance of the defenses that his belief will subsequently be exposed to strong attack versus making no such announcement" (1962, pg 26). They theorized that an additional belief-threatening manipulation such as that used in inoculation could stimulate persuasive defense. "The notion is that subjects use the period following the warning but preceding the message to consider arguments supporting their own position and refuting antagonistic positions" (Petty & Cacioppo, 1977, pg 645).

In an experiment which tested a forewarned group compared to an unwarned group, McGuire & Papageorgis found statistically significant evidence that warning subjects that their beliefs would be attacked enhances the effectiveness of refutational defenses such as inoculation. Following this, a series of experiments by Richard Petty and John Cacioppo would show evidence that anticipatory counterargumentation does in fact mediate the resistance to persuasion conveyed by forewarning (1977). Interestingly though, forewarning in the absence of refutational defense was found to make subjects more susceptible to persuasion. It is theorized that this is due to an anticipatory shift toward a moderate position. The motive in the absence of strong counterargument is one of self presentation and dissonance reduction. To this end, Petty & Cacioppo state that "A moderate position on the topic is adopted because it is easier to defend and/or gives the appearance of open- and broad-mindedness" (1977, pg 646). "Hence, on occasions when we wish a person to maintain his beliefs at a high level but are unable to defend these beliefs in advance, it might be unwise to threaten that his beliefs may be attacked. But

when there will be an opportunity to defend the beliefs in advance, then, as has been demonstrated, it is wise to forewarn the person of the possibility of attack before the defenses are presented" (McGuire & Papageorgis, 1962, pg 32-33).

As with the case of inoculation, the author believes that the tenets of forewarning provide another unique mitigation strategy to the social engineering threat. As Petty & Cacioppo state "When anticipating a discrepant communication…a person forewarned is forearmed!" (1977, pg 654). The application of a forewarning strategy should be implemented with discretion though as one could accidentally invoke susceptibility instead of a resistance effect. A social engineering forewarning strategy should be employed only in the presence of refutational defense training as the empirical evidence suggests.

5.5 Metacognition

Metacognition can be defined as the awareness of one's own thinking and cognitive processes, that is, thinking about thoughts. Two psychologists from The Ohio State University, Zakary Tormala & Richard Petty put forth a metacognitive approach for understanding resistance to persuasion (Tormala & Petty, 2002). Within this construct, they examined the effects resisting persuasion has on attitude certainty; the extent to which a person views his or her attitude as correct. Specifically, they tested the position that when people resist persuasion they become more confident in their initial attitudes. This is important because conviction to beliefs has shown to predict future behavior. To this end, Tormala & Petty state that "The primary reason researchers have been interested in attitude certainty over the years is that certainty has been shown to have a number of

important consequences. For example, the more certain people are of their attitudes, the more these attitudes tend to guide behavior, resist persuasion, and persist over time" (2004, pg 428).

In a series of experiments, Tormala & Petty demonstrated that when participants resisted persuasive attempts, their attitude certainty increased. Their theory proposes "a metacognitive account of this phenomenon, whereby people think about their own resistance and draw corresponding (attributional) inferences about their attitudes…when people perceive that they have resisted persuasion successfully, they might infer that their attitude is correct, or valid, and thus feel more certain about it" (2002, pg 1298). In addition, they found that an increase in attitude certainty makes initially held beliefs more resistant to later attacks and more predictive of behavioral intent (2002).

Traditionally, the resisting of persuasion has been the end state of previous research. Tormala & Petty's theory of metacognition shows that resistance can play a mediating role to other less obvious effects. In this way, the role of metacognition as applied to the resistance of social engineering could be used to increase attitude certainty about information security policies. As such, the author hypothesizes that if a social engineering resistance program incorporated the opportunity to resist a variety of persuasive social engineering tactics, attitude certainty about those policies would increase. According to this theory, this would predict behavior in accordance with that policy, an increase in resistance to persuasive attempts against those beliefs, and a persistence of these attitudes over time.

5.6 Illusion of Invulnerability

A group of psychologists including Brad Sagarin, the aforementioned Robert Cialdini, William Rice, and Sherman Serna conducted a series of three experiments that set out to examine the efficacy of a treatment designed to encourage resistance to illegitimate persuasion; those based upon deceptive techniques. They theorized that as people are naturally resistant to attempts at deception because of evolved tendencies to avoid trickery; this natural resistance could be evoked in those that were given rule sets for distinguishing between legitimate and illegitimate attempts at persuasion (2002). To test this in an initial experiment, they had subjects try to discriminate between legitimate and illegitimate authority-based advertisements after learning rule sets for distinguishing between the two. The results of this study demonstrated that this type of treatment did significantly reduce the persuasiveness of illegitimate authority-based appeals and may have theoretical applications to illegitimate social engineering attempts.

In a second study, Sagarin et al. aimed to extend these results by having subjects rate the advertisements several days after the treatment was given. This study showed that resistance in fact "generalized to novel exemplars, persisted over time, and appeared outside of the laboratory context" (pg 526). These findings are especially relevant to this research as they demonstrate that an illegitimate persuasion treatment for social engineering appeals may exhibit the same temporal and generalizable effects.

In addition to these results, there was an unexpected finding in the second study that "although participants receiving the treatment rated the ads containing legitimate authorities as significantly more persuasive, as compared with controls, they did not resist the ads containing illegitimate authorities more effectively than did controls" (pg 533).

The researchers theorized that "these results suggest that participants may have agreed with the characterization of illegitimacy presented in the treatment but may not have acted on it because they were not susceptible to it" (pg 533). In a subsequent pilot study, the researchers went on to confirm that subjects who received the treatment maintained perceptions of personal invulnerability and were thus unmotivated to use defenses against the advertisements. This finding provides an explanation as to why current policy and awareness training programs have been partially ineffective for defending against social engineering attacks.

Personal invulnerability is a well known psychological phenomenon and includes constructs such as the optimism bias and superiority bias wherein people tend to overestimate positive outcomes of their own behavior relative to others. "Such illusions of unique invulnerability are widespread, leading at times to harmful or even fatal results. In the area of health psychology, the optimistic bias appears as a discrepancy between perceptions of others' susceptibility to a disease and perceptions of one's own personal susceptibility to the illness. This bias can lead to negative health outcomes, as low levels of perceived personal susceptibility are associated with poor compliance with preventative health behaviors" (Sagarin et. al, 2002, pg 533).

Much in the same way, Kevin Mitnick states that "many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication devices such as time-based tokens or biometric smart cards. Anyone who thinks that security products alone offer true security is settling for the illusion of security" (2003, pg 2). As such, the lessons learned

from health psychology about dispelling illusions of invulnerability show great promise to the application of resisting persuasion and more specifically to developing social engineering training programs.

In the last of their experiments, Sagarin et al. aimed to dispel this illusion of invulnerability by demonstrating to participants that they could be fooled. To do this they had the participants indicate in writing how convincing advertisements were before being shown the underlying deception. "Participants who made a written commitment as to their assessment of the ad were faced with the undeniable realization that the ad had not merely tried to fool them, it had succeeded. With their illusions of invulnerability dispelled, participants acquired a strong motivation to avoid being fooled again" (pg 539). This study showed that to confer strong resistance to persuasion, it is not sufficient to just provide awareness that people in general can be deceived, people must learn that they are personally vulnerable to the threat.

The experiments conducted by Sagarin et al. "demonstrate that attempts to confer resistance to appeals will likely be successful to the extent that they install 2 conceptual features: perceived undue manipulative intent of the source of the appeal and perceived personal vulnerability to such manipulation" (Sagarin et al, 2002, pg 526). These findings have a hypothetical impact to the application of training programs built to instill resistance to social engineering attempts. Successful training should incorporate an element that moves beyond informing personnel about their vulnerabilities as is commonly done with awareness training to that of personally demonstrating that vulnerability. In addition, providing people with rule sets to recognize illegitimate or

manipulative attempts at persuasion will empower their natural tendency to resist persuasion because of evolved tendencies to avoid deception.

In addition to these insights, the authors state that "the present treatment was tested in the context of authority-based advertisements, but the technique could be applied readily to other persuasive techniques. For example, many advertisements use scarcity in an effort to increase the desirability of the product. Such scarcity-based appeals could be distinguished between those that use scarcity legitimately and those that use it illegitimately" (2002, pg 539). This implies that the use of perceived manipulation and personal vulnerability could also be theoretically applied across the model of social engineering presented in Chapter IV.

VI. CONCLUSION

"The state produced in the laboratory may be likened to a light doze compared to the profound slumber induced by the prepotent authority system of a national government"

–Stanley Milgram

The mission of the Unites States Air Force is to fly, fight, and win… in air, space, and cyberspace. To achieve that mission, the Air Force has a vision based on three core competencies, one of which is developing Airmen. Through an exploration of the issues and concepts provided by this research, it is clear that addressing the human factor in information security will no doubt be a crucial enabler to the success of the Air Force's distinctive capabilities, especially that of information superiority.

6.1 Impact on the Air Force

The driving force behind this study was a research question developed with an impact on the Air Force directly in mind. That is, how can the Air Force protect its personnel from the increasing information security threat of social engineering? This research has shown that the answer lies in a paradigm shift away from the current practice of reactionary hardware, software, and policy patches toward that of proactively addressing the wetware. Or said another way consistent with one of the Air Force core competencies; Developing Airmen.

In addressing this initial research question, several other investigative questions were answered by formally demonstrating a relationship between the deceptive techniques of social engineering and a body of research on persuasion. By establishing this link, novel insights on how people can be protected from techniques of social engineering emerged. If these insights can be thoroughly tested and implemented into Air Force training programs successfully, the impact would be commensurate with avoiding the consequences of recent human-mediated incidents such as the CENTCOM breach, the Stuxnet worm, and the WikiLeaks case. In the meantime, this research impacts the Air Force by clearly demonstrating the threat of social engineering and the value of human-centric information security.

6.2 Limitations of this Work

Due to the time and resource constraints placed on academic endeavors such as this work, there are certain limitations to its extensibility. The current research is primarily an intellectual exercise based upon an in depth exploration of the literature and a qualitative analysis that establishes formal relationships for hypothesis building. Although a new framework and several hypotheses are put forth in this research, the opportunity to collect quantitative data in an effort to test those hypotheses in an experimental setting remains an aspiration for the future. As such, the real world application of this research remains theoretical in nature.

6.3 Areas for Future Study

As previously stated, one of the intended objectives of this effort was to build a foundation upon which further laboratory-based experimental research could be conducted. During the course of this research, four methods that have been shown to develop resistance to persuasion have been discussed; inoculation, forewarning, metacognition, and the illusion of invulnerability. Individually, they are presented as unique approaches to mitigating the threat of social engineering. Together, they could form the basis of novel training programs aimed at protecting the human element of information security. To validate these hypotheses in an experimental setting, a researcher could take a baseline measure of a population's receptiveness to persuasive social engineering attempts, and compare that measure to samples taken after one or more of these four resistance treatments are given. Quantifying those treatment effects would give new insights into how to employ novel resistance training programs.

Beyond these hypotheses, new research questions surfaced based upon the insights of the analysis and include; how do these four different resistance treatments correlate with the eight psychological enablers of social engineering identified in the analysis? What are the optimal combinations of these resistance treatments for specific population subsets? What are the optimal training lengths and delivery methods for targeting certain types of social engineering attacks? If a treatment that successfully bolsters resistance to persuasion such as those mentioned above is given to personnel, what would be the duration effects of that treatment? Based on that information then, what is the optimal training interval for such resistance treatments? Given the rapidly

evolving cyber landscape, how do different technologies or information delivery devices mediate these constructs of persuasion, influence, trust, and the like?

In summary, there are many unexplored research vectors in human-centric information security that deserve consideration and could provide potential benefit to the Air Force as well as any other enterprise that depends upon information to accomplish their mission.

6.4 Closing Thought

The Air Force's most valuable asset has always been and will always be its people. Research into the development of the human factor holds the key to protecting that asset as well as the second most valuable asset of the Air Force; its information. As the U.S. Deputy Secretary of Defense stated in response to one of the recent Air Force information security incidents; "it serves as an important wake-up call" (2010). We'll see who listens.

BIBLIOGRAPHY

Allen, M. (2007). Social Engineering: A Means to Violate a Computer System. *SANS Institute InfoSec Reading Room,* retrieved from: http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529.

Bickman, L. (1974). The Social Power of a Uniform. *Journal of Applied Social Psychology*, 4, 47-61.

Cialdini, R. B. (2006). *Influence: The Psychology of Persuasion.* New York: Harper Publishing.

Cialdini, R. B. (2008). *Influence:* Harnessing the Science of Persuasion. Harvard Business Review, 79, 72-79.

Crain, J. O. (2010). Fighting Phishing with Trusted Email. *International conference on Availability, Reliability and Security.* Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5438053&tag=1.

[Ebay phishing email: untitled image]. Retrieved May 6, 2011 from: http://www.homesfornh.com/internet/images/ebay-2.JPG

Lynn, W. J. III (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, September/October, retrieved from: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Markoff, J. (2011, February 11). Malware Aimed at Iran Hit Five Sites, Report Says. *The New York Times*. Retrieved from: http://www.nytimes.com/2011/02/13/science/13stuxnet.html

McGuire, W. J. (1964). Inducing Resistance to Persuasion: Some Contemporary Approaches. *Experimental Social Psychology* , 191-229.

McGuire, W. J. (1961). Resistance to Persuasion Conferred by Active and Passive Prior Refutation of the Same and Alternative Counterarguments. *Journal of Abnormal and Social Psychology* , 63(2), 326-332.

McGuire, W. J. & Papageorgis, D. (1962). Effectiveness of Forewarning in Developing Resistance to Persuasion. *Public Opinion Quarterly*, 26 (1), 24-34.

Microsoft Corporation. (2008). *Microsoft Security Intelligence Report Volume 6.* Microsoft Corporation. retrieved from: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=aa6e0660-dc24-4930-affd-e33572ccb91f&displaylang=en

Milgram, S. (1963). Behavioral Study of Obedience. *Journal of Abnormal and Social Psychology*, 67 (4), 371-378.

Milgram, S. (1973). The Perils of Obedience. *Harper's Magazine*, 62-77.

[Milgram experiment: untitled image]. Retrieved May 6, 2011 from: http://sites.google.com/site/ibpsychology/300px-Milgram_experiment.png

Mitnick, K. D. (2003). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis: Wiley Publishing.

Mitnick, K. D. & Simon, W. L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers.* Indianapolis: Wiley Publishing.

Nakashima, E. (2010, August 24). Defense official discloses cyberattack. *The Washington Post* . Retrieved from:http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html?hpid%3Dtopnews&sub=AR.

Petty, R. E. & Cacioppo (1977). Forewarning, Cognitive Responding, and Resistance to Persuasion. *Journal of Personality and Social Psychology* , 35 (9), 645-655.

Pfau, M. & Szabo, E. (2003). Inoculation and Resistance to Persuasion. In Seiter, J. & Glass, R. (Eds.), Perspectives on Persuasion, Social Influence, and Compliance Gaining (pg 265-286). Needham Heights, MA: Allyn & Bacon.

Pipkin, D. L. (2000). *Information Security: Protecting the Global enterprise.* Upper Saddle River, New Jersey: Prentice Hall, Inc.

Rush, J. J. (1999). The "Social Engineering" of Internet Fraud. *Internet Society's INET'99 Conference.* Retrieved from: http://www.isoc.org/inet99/proceedings/3g/3g_2.htm.

Sagarin, B. J., Cialdini, R. B., Rice, W. E., & Serna, S. B. (2002). Dispelling the Illusion of Invulnerability: The Motivations and Mechanisms of Resistance to Persuasion. *Journal of Personality and Social Psychology*, 83(3), 526-541.

Savage, C. (2010). U.S. Tries to Build Case for Conspiracy by WikiLeaks. *The New York Times,15 December,* Retrieved from: http://www.nytimes.com/2010/12/16/world/16wiki.html?_r=2&pagewanted=print.

Secretary of the Air Force (2010). Cyberspace Operations. *Air Force Doctrine Document 3-12.* Retrieved from: http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf.

Secretary of the Air Force (2005). Information Operations. *Air Force Doctrine Document 2-5.* Retrieved from: http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-13.pdf.

[SET screenshot: untitled image]. Retrieved May 6, 2011 from: http://media.photobucket.com/image/recent/1-VIP-/55de078f.png

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2), 237-246.

Thomas, T. L. (2008). Cyberskepticism: The Mind's Firewall. *IOSPHERE Spring* , 4-8.

Thornburgh, T. (2005). Social Engineering: The Dark Art. *InfoSec Conference 2004* (pp. 133-135). ACM.

Tormala, Z. L. & Petty, R. E. (2002). What Doesn't Kill Me Makes Me Stronger: The Effects of Resisting Persuasion on Attitude Certainty. *Journal of Personality and Social Psychology* , 1298-1313.

Tormala, Z. L. & Petty, R. E. (2004). Source Credibility and Attitude Certainty: A Metacognitive Analysis of Resistance to Persuasion. *Journal of Consumer Psychology* , 14(4), 427-442.

Treasury Inspector General for Tax Administration (2007). Employees Continue to be Susceptible to Social Engineering Attempts That Could Be Used by Hackers.

Memorandum for Chief, Mission Assurance and Security Services, Retrieved from: http://www.treasury.gov/tigta/auditreports/2007reports/200720107fr.pdf.

United States Department of Justice. (1999). *Kevin Mitnick Sentenced to Nearly Four Years in Prision: Computer Hacker Ordered to Pay Restitution to Victim Companies Whose Systems Were Compromised.* U.S. Attorney's Office Central District of California, Press Release, 9 August. Retrieved from: http://www.justice.gov/criminal/cybercrime/mitnick.htm

Vita

Alexander D. Nelson graduated from Centerville High School, Centerville, Ohio in 1996. Immediately following, he entered undergraduate studies at Wright State University, Dayton, Ohio where he graduated with a Bachelor's Degree in Psychology in 2001.

Upon graduation, Alexander was employed by Wright State as a researcher in the Department of Psychology conducting research on game-based, distributed team training protocols under a Multi-University Research Initiative (MURI). In 2003 while continuing as a part time researcher in the MURI laboratory, Mr. Nelson entered into the Department of Psychology's Master's program majoring in Human Factors Engineering with a minor in Industrial/Organizational Psychology.

In 2004, Mr. Nelson began his current occupation with the Air Force Research Laboratory (AFRL), Human Effectiveness Directorate, Wright-Patterson AFB. In this appointment at AFRL, Alexander has served as a research psychologist and program manager for various Air Force acquisitions and research efforts.

In 2010, Alexander entered into the Cyber Warfare program of the Department of Electrical and Computer Engineering at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. Mr. Nelson has focused his research on the psychological foundations of influence and persuasion as they pertain to information security and will graduate in 2011 returning to AFRL.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
16-Jun-2011	Graduate Research Project	14 May 2010 – 16 Jun 2011

4. TITLE AND SUBTITLE

Patching the Wetware: Addressing the Human Factor in Information Security

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Alexander D. Nelson

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology - Graduate School of Engineering and Management
2950 Hobson Way
Wright Patterson Air Force Base, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/ICW/ENG/11-11

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
INTENTIONALLY LEFT BLANK

10. SPONSOR/MONITOR'S ACRONYM(S)
INTENTIONALLY LEFT BLANK

11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States

14. ABSTRACT

In the practice of information security, it is increasingly observed that the weakest link in the security chain is the human operator. A reason often cited for this observation is that the human factor is simpler and cheaper to manipulate than the complex technological protections of digital information systems.

Current anecdotes where the human was targeted to undermine military information protection systems include the 2008 breach of USCENTCOM computer systems with a USB device, and the more recent 2010 compromise of classified documents published on the WikiLeaks website. These infamous cases, among others, highlight the need for more robust human-centric information security measures to mitigate the risks of social engineering.

To address this need, this research effort reviewed seminal works on social engineering and from the social psychology literature in order to conduct a qualitative analysis that establishes a link between the psychological principles underlying social engineering techniques and recognized principles of persuasion and influence. After this connection is established, several theories from the social psychology domain on how to develop resistance to persuasion are discussed as they could be applied to protecting personnel from social engineering attempts. Specifically, the theories of inoculation, forewarning, metacognition, and dispelling the illusion of invulnerability are presented as potential defenses.

15. SUBJECT TERMS
Social Engineering, Information Security, Social Psychology, Influence, Persuasion, Inoculation,

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Robert F. Mills, PhD (ENG)
U	U	U	UU	80	**19b. TELEPHONE NUMBER** *(Include area code)* (937)257-3636x4527 robert.mills@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18